Protecting data passing between data processing device and terminal device connected via telecommunications network

Patent Number: DE4442357
Publication date: 1996-06-05
Inventor(s): BOEHL PETER (DE); KORST UWE K H (DE)
Applicant(s):: DEUTSCHE TELEKOM AG (DE)
Requested Patent: ☐ DE4442357
Application Number: DE19944442357 19941129
Priority Number(s): DE19944442357 19941129
IPC Classification: H04L9/32
EC Classification: H04L9/32, G07F7/10D4E2
Equivalents:

Abstract

The method involves using a code stored in a security module in each device for mutual authentication before commencing the transfer of data. Each code represents keys within an algorithm which processes random data fed to the terminal or data processor; the results of the processing are fed back to the data processor or terminal.The data are integrally protected when the code arrives, is stored in the terminal and transmitted using a message authentication code or MAC with the aid of algorithms and keys in each security module. Secure counters in the security modules perform additional monitoring of the data protected by the MAC.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 44 42 357 A 1**

(51) Int. Cl.[6]: **H 04 L 9/32**

(21) Aktenzeichen: P 44 42 357.8
(22) Anmeldetag: 29. 11. 94
(43) Offenlegungstag: 5. 6. 96

DE 44 42 357 A 1

(71) Anmelder:
Deutsche Telekom AG, 53175 Bonn, DE

(74) Vertreter:
Gornott, D., Dipl.-Ing., Pat.-Anw., 64291 Darmstadt

(72) Erfinder:
Boehl, Peter, 64331 Weiterstadt, DE; Korst, Uwe K. H., 64625 Bensheim, DE

(56) Entgegenhaltungen:

DE	43 17 380 C1
DE	41 38 861 A1
US	50 48 085
EP	05 73 245 A2

US-Z.: WOO, T.Y.C. et al.: Authentication for Distibuted Sysems. In: Computer, Januar 1992, S 39-52;

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren und Anordnung zur Sicherung von Daten

(57) Bei einem Verfahren und einer Anordnung zur Sicherung von Daten im Verkehr zwischen einer Datenverarbeitungseinrichtung und einem Endgerät, die miteinander über ein Telekommunikationsnetz verbunden sind, erfolgt vor der Aufnahme der Übertragung von Daten eine gegenseitige Authentifikation unter Verwendung von in jeweils einem Sicherheitsmodul in der Datenverarbeitungseinrichtung und im Endgerät gespeicherten Codes.

DE 44 42 357 A 1

Beschreibung

Die Erfindung betrifft ein Verfahren und eine Anordnung zur Sicherung von Daten im Verkehr zwischen einer Datenverarbeitungseinrichtung und einem Endgerät, die miteinander über ein Telekommunikationsnetz verbunden sind.

Je größer und komplexer Telekommunikationsnetze mit den daran angeschlossenen Einrichtungen sind und je mehr Kommunikationspartner untereinander Daten austauschen, umso größer wird die Gefahr, daß entweder unberechtigte Personen sich Zugang verschaffen oder berechtigte Personen (beispielsweise die Betreiber einer Kommunikationsstelle) vorsätzlich oder ungewollt unzulässige Einstellungen vornehmen. Deshalb sind Daten einschließlich derjenigen Daten, welche Programme betreffen, sowohl während der Übertragung als auch während der nachfolgenden Speicherung gegen Veränderungen zu schützen.

Bei einer Datenübertragung ist es daher erforderlich, daß sich beide Partner von der Authentizität des jeweils anderen Partners überzeugen, um zu verhindern, daß unberechtigte Kommunikationspartner sensitive Daten erhalten oder manipulierte Daten eingeben. Ferner ist es erforderlich, daß in Endgeräten eines Telekommunikationsnetz es Veränderungen an sensitiven Daten durch Unbefugte erkannt werden.

Aus DE 42 26 617 A1 ist ein Verfahren und eine Anordnung zur wahlweisen Anschaltung von über maschinenlesbaren Karten betriebenen Endgeräten bekannt. Dabei erhalten diese Endgeräte (Kartentelefone) die für den Betrieb erforderlichen Daten und Programme über eine Datenverarbeitungseinrichtung und das Telekommunikationsnetz. Die Endgeräte übertragen auch Daten zur Datenverarbeitungseinrichtung. Bei diesem bekannten Verfahren sind die übertragenen Daten nicht gegen Manipulation gesichert. Außerdem besteht nach der Entstehung und bei der Speicherung der Daten die Gefahr, daß manipulierte Daten bei dem jeweiligen Empfänger nicht erkannt werden.

Aufgabe der Erfindung ist es daher, im Verkehr zwischen einer Datenverarbeitungseinrichtung und einem Endgerät, die miteinander über ein Telekommunikationsnetz verbunden sind, eine unberechtigte Einflußnahme auf die zu übertragenden und auf die gespeicherten Daten zu verhindern.

Diese Aufgabe wird bei dem erfindungsgemäßen Verfahren dadurch gelöst, daß vor der Aufnahme der Übertragung von Daten eine gegenseitige Authentifikation unter Verwendung von in jeweils einem Sicherheitsmodul in der Datenverarbeitungseinrichtung und im Endgerät gespeicherten Codes erfolgt.

Mit dem erfindungsgemäßen Verfahren wird sichergestellt, daß ein Austausch von Daten nur zwischen der berechtigten Datenverarbeitungseinrichtung und den berechtigten Endgeräten stattfinden kann. Als Codes zur gegenseitigen Authentifikation können verschiedene geeignete Codes verwendet werden, vorzugsweise ist jedoch bei dem erfindungsgemäßen Verfahren vorgesehen, daß die Codes jeweils Schlüssel innerhalb eines Algorithmus darstellen, mit welchem dem Endgerät bzw. der Datenverarbeitungseinrichtung zugeführte Zufallsdaten verarbeitet werden, und daß das Ergebnis der Verarbeitung jeweils zur Datenverarbeitungseinrichtung bzw. zum Endgerät rückübertragen wird.

Gemäß einer Weiterbildung des erfindungsgemäßen Verfahrens ist eine Sicherung der zu übertragenden Daten dadurch möglich, daß die Daten bei der Entstehung, Speicherung im Endgerät und Übertragung durch Nachrichten-Authentifikations-Codes (MAC) mit Hilfe von in den jeweiligen Sicherheitsmodulen abgelegten Algorithmen und Schlüsseln integritätsgesichert werden.

Eine weitere Verbesserung der Sicherung der zu übertragenden Daten ist bei dem erfindungsgemäßen Verfahren dadurch möglich, daß Zähler in den Sicherheitsmodulen gesichert geführt werden, die eine zusätzliche Kontrolle der durch die Nachrichten-Authentifikations-Codes gesicherten Daten ergeben.

Die der Erfindung zugrundeliegende Aufgabe wird bei einer gattungsgemäßen Anordnung dadurch gelöst, daß in der Datenverarbeitungseinrichtung und im Endgerät Sicherheitsmodule vorgesehen sind, in welchen Codes zur gegenseitigen Authentifikation ablegbar sind.

Eine Weiterbildung der erfindungsgemäßen Anordnung besteht darin, daß in den Sicherheitsmodulen ferner Codes zur Sicherung der Integrität und Authentizität der zu übertragenden Daten ablegbar sind. Vorzugsweise ist dabei vorgesehen, daß die Sicherheitsmodule fernladbar ausgebildet sind. Dies hat den Vorteil, daß die Codes in den Sicherheitsmodulen bei Bedarf geändert werden können, ohne daß an den Sicherheitsmodulen selbst durch geeignetes Personal Arbeiten durchgeführt werden müssen.

Bei einer anderen Weiterbildung der erfindungsgemäßen Anordnung sind als Sicherheitsmodule Chipkarten in Form von Einschubmodulen vorgesehen. Dieses hat den Vorteil, daß die bereits auf Chipkarten implementierten Funktionalitäten in einfacher Weise für das erfindungsgemäße Verfahren oder bei der erfindungsgemäßen Anordnung benutzt werden können.

Die Erfindung ist an sich für verschiedenartige Endgeräte geeignet. Eine besonders vorteilhafte Anwendung besteht jedoch darin, daß das Endgerät ein Kartentelefon ist.

Ein Ausführungsbeispiel der Erfindung ist in der Zeichnung anhand mehrerer Figuren dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt

Fig. 1 ein Blockschaltbild einer erfindungsgemäßen Anordnung,

Fig. 2 ein Ablaufdiagramm zur Erläuterung der Authentifikation der Datenverarbeitungseinrichtung und des Endgerätes und

Fig. 3 ein Ablaufdiagramm zur Erläuterung der Sicherung der Datenintegrität und Datenauthentizität.

Bei dem in **Fig. 1** dargestellten Ausführungsbeispiel ist ein Endgerät **1**, das mit einer Chipkarte **2** betreibbar ist, an ein Telekommunikationsnetz **3** angeschlossen. Das Endgerät **1** kann beispielsweise ein Kartentelefon oder eine Telefaxstation sein, die der Kunde mit einer Chipkarte in Betrieb nimmt, worauf mit dem Endgerät **1** über das Telekommunikationsnetz **3** mit beliebigen anderen in der Zeichnung nicht dargestellten Endgeräten Nachrichten ausgetauscht werden können. Es können eine Vielzahl von Kartenvarianten eingesetzt werden — beispielsweise Telefonkarten, Buchungskarten, Kooperationskarten, elektronische Geldbörsen.

Bei der Benutzung des Endgerätes **1** mit der Chipkarte **2** entstehen sogenannte Nutzungsdaten, die gesichert gespeichert werden müssen. Diese Daten enthalten beispielsweise Transaktionsdatensätze, die für eine spätere Abrechnung verwendet und dazu von Zeit zu Zeit, beispielsweise alle 24 Stunden, über das Telekommunikationsnetz **3** zu einer Datenverarbeitungseinrichtung **4** übertragen werden.

Das Endgerät 1, beispielsweise ein Kartentelefon, ist mit einem internen steckbaren Sicherheitsmodul 5 ausgestattet und kann nur zusammen mit diesem aktiviert werden. Das Sicherheitsmodul enthält im wesentlichen einen nichtflüchtigen Speicher für die veränderlichen Daten, einschließlich der Schlüssel, Ein- und Ausgangsschnittstellen und einen Mikrocomputer zur Anwendung von gespeicherten Algorithmen auf zugeführte Daten und zur Steuerung des Sicherheitsmoduls.

Nach der Installation eines Endgerätes ist es erforderlich, eine Verbindung mit der Datenverarbeitungseinrichtung 4 aufzunehmen, um das Endgerät 1 mit Programmen und den für den Betrieb erforderlichen Parametern zu versorgen. Dabei werden alle sicherheitsrelevanten Parameter im Sicherheitsmodul 5 gespeichert. In dem dargestellten Beispiel handelt es sich dabei um einen Schlüssel K1 zur Authentifikation des Endgerätes, einen Schlüssel K2 zur Erzeugung eines Nachrichten-Authentifikations-Codes. Der Algorithmus f ist bei dem Ausführungsbeispiel im Sicherheitsmodul fest gespeichert, kann im Rahmen der Erfindung jedoch auch veränderbar sein.

In ähnlicher Weise ist in der Datenverarbeitungseinrichtung 4 ein Sicherheitsmodul 6 angeordnet, in welchem ebenfalls Parameter und Algorithmen gespeichert sind.

Nach der beschriebenen Installation des Endgerätes kann es benutzt werden. Dabei entstehen die oben erwähnten Nutzungsdaten, die gesichert gespeichert werden. Dazu werden geeignete Zähler im Sicherheitsmodul 5 inkrementiert und Datensätze im Endgerät 1 gebildet. Diese Datensätze werden mit einem MAC versehen, um Manipulation zu erkennen. Nach einem vorgegebenen Zeitraum, beispielsweise nach 24 Stunden, erfolgt ein Datenaustausch mit der Datenverarbeitungseinrichtung 4.

Fig. 2 zeigt die nach einem an sich bekannten Verfahren erfolgende Authentifikation des Endgerätes 1 und der Datenverarbeitungseinrichtung 4. Dazu wird zunächst im Sicherheitsmodul 6 der Datenverarbeitungseinrichtung 4 bei 11 eine Zufallszahl RAND erzeugt und über die Datenverarbeitungseinrichtung 4, das Telekommunikationsnetz 3 und das Endgerät 1 dem Sicherheitsmodul 5 des Endgerätes zugeführt. Dort wird anhand des gespeicherten Schlüssels K1 und des Algorithmus f_{K1} ein Authentifikationsparameter AP2 berechnet (12), der wieder an das Sicherheitsmodul 6 übertragen wird. Parallel dazu wird im Sicherheitsmodul 6 mit der gleichen Zufallszahl und dem gleichen Algorithmus f_{K1} ein Authentifikationsparameter AP1 berechnet (13). Beide Authentifikationsparameter werden dann verglichen (14). Bei Gleichheit ist das Endgerät 1 authentifiziert, bei Ungleichheit nicht. Ein entsprechendes Verfahren mit den Schritten 15 bis 18 läuft dann in der Gegenrichtung ab und führt dazu, daß zutreffendenfalls dem Endgerät die Echtheit der Datenverarbeitungseinrichtung 4 bekannt wird.

Die Authentizität und die Integrität der gespeicherten und zu übertragenden Daten werden gemäß **Fig. 3** überprüft. Sowohl im Sicherheitsmodul 5 als auch im Sicherheitsmodul 6 ist ein Schlüssel K2 abgelegt. Dem Sicherheitsmodul 5 wird der zu speichernde und später zu übermittelnde Datensatz (Nachricht M) mit der Entstehung 21 im Endgerät 1 zugeführt und bei 22 mit dem Algorithmus f mit dem Schlüssel K2 zu einem Nachrichten-Authentifikations-Code MAC verarbeitet, der zusammen mit dem Datensatz M bei 23 im Endgerät 1 gespeichert wird. Gleichzeitig wird im Sicherheitsmodul 5 ein Zähler 24 inkrementiert. Nach entsprechend häufiger Benutzung des Endgerätes 1 befinden sich im Speicher des Endgerätes n Datensätze. Außerdem weist der Zähler 24 den Zählerstand n auf.

Zur Abfrage der Datensätze aus dem Speicher des Endgerätes 1 wählt die Datenverarbeitungseinrichtung 4 das Endgerät 1 an, worauf eine Authentifikation gemäß **Fig. 2** erfolgt. Ist diese erfolgreich abgeschlossen, werden die bei 23 im Endgerät 1 gespeicherten Datensätze einschließlich der MACs und der Zählerstand des Zählers 24 zur Datenverarbeitungseinrichtung 4 übertragen. Jeweils ein empfangener Datensatz M* und der dazugehörige MAC* werden in das Sicherheitsmodul 6 bei 25 eingegeben. Bei 27 wird unter Verwendung des Algorithmus f_{K2} aus dem empfangenen Datensatz M* ein Nachrichten-Authentifikations-Code MAC** abgeleitet. Dieser wird bei 27 mit dem empfangenen MAC* verglichen. Bei Gleichheit steht fest, daß die bei der Benutzung des Endgerätes entstandenen Datensätze weder im Speicher des Endgerätes noch bei der Übertragung bis zur Datenverarbeitungseinrichtung verändert wurden.

Beim Empfang der Datensätze bzw. bei deren Einschreiben in das Sicherheitsmodul 6 werden die Datensätze gezählt. Ihre Anzahl n* wird dann zusammen mit dem übertragenen Zählerstand n bei 28 in das Sicherheitsmodul eingelesen und bei 29 verglichen. Bei Gleichheit steht fest, daß keiner der bei der Benutzung des Endgerätes 1 entstandenen Datensätze gelöscht oder dupliziert worden ist. Der Zählerstand n kann auch durch einen MAC gesichert übertragen werden.

Patentansprüche

1. Verfahren zur Sicherung von Daten im Verkehr zwischen einer Datenverarbeitungseinrichtung und einem Endgerät, die miteinander über ein Telekommunikationsnetz verbunden sind, **dadurch gekennzeichnet**, daß vor der Aufnahme der Übertragung von Daten eine gegenseitige Authentifikation unter Verwendung von in jeweils einem Sicherheitsmodul in der Datenverarbeitungseinrichtung und im Endgerät gespeicherten Codes erfolgt.
2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Codes jeweils Schlüssel innerhalb eines Algorithmus darstellen, mit welchem dem Endgerät bzw. der Datenverarbeitungseinrichtung zugeführte Zufallsdaten verarbeitet werden, und daß das Ergebnis der Verarbeitung jeweils zur Datenverarbeitungseinrichtung bzw. zum Endgerät rückübertragen wird.
3. Verfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß die Daten bei der Entstehung, Speicherung im Endgerät und Übertragung durch Nachrichten-Authentifikations-Codes (MAC) mit Hilfe von in den jeweiligen Sicherheitsmodulen abgelegten Algorithmen und Schlüsseln integritätsgesichert werden.
4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß Zähler in den Sicherheitsmodulen gesichert geführt werden, die eine zusätzliche Kontrolle der durch die Nachrichten-Authentifikations-Codes gesicherten Daten ergeben.
5. Anordnung zur Sicherung von Daten im Verkehr zwischen einer Datenverarbeitungseinrichtung und einem Endgerät, die miteinander über ein Telekommunikationsnetz verbunden sind, dadurch gekennzeichnet, daß in der Datenverarbeitungseinrich-

tung (4) und im Endgerät (1) Sicherheitsmodule (6, 4) vorgesehen sind, in welchen Codes zur gegenseitigen Authentifikation ablegbar sind.

6. Anordnung nach Anspruch 5, dadurch gekennzeichnet, daß in den Sicherheitsmodulen (6, 4) ferner Codes zur Sicherung der Integrität und Authentizität der zu übertragenden Daten ablegbar sind.

7. Anordnung nach einem der Ansprüche 5 oder 6, dadurch gekennzeichnet, daß die Sicherheitsmodule (6, 4) fernladbar ausgebildet sind.

8. Anordnung nach einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, daß als Sicherheitsmodule Chipkarten in Form von Einschubmodulen vorgesehen sind.

9. Anordnung nach einem der Ansprüche 5 bis 8, dadurch gekennzeichnet, daß das Endgerät (1) ein Kartentelefon ist.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 44 42 357 A1
Int. Cl.[6]: H 04 L 9/32
Offenlegungstag: 5. Juni 1996

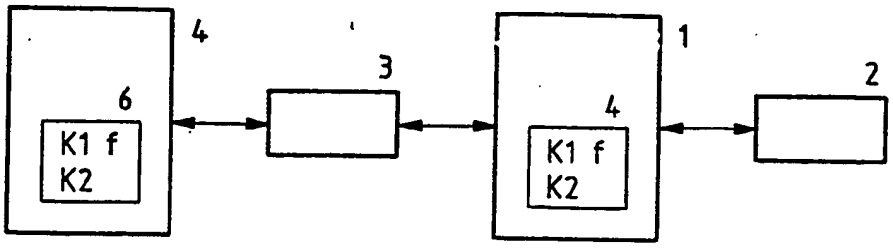

Fig.1

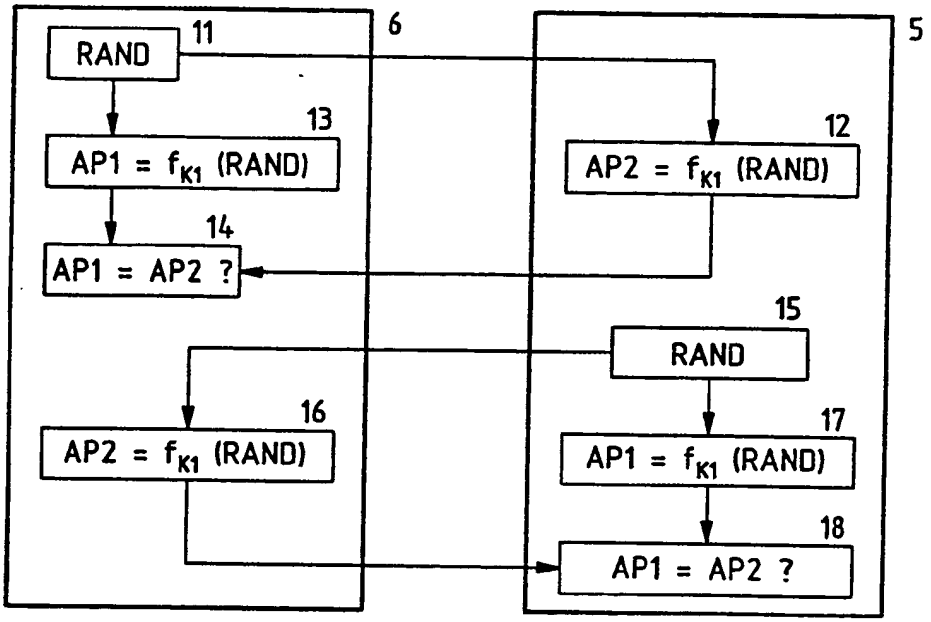

Fig.2

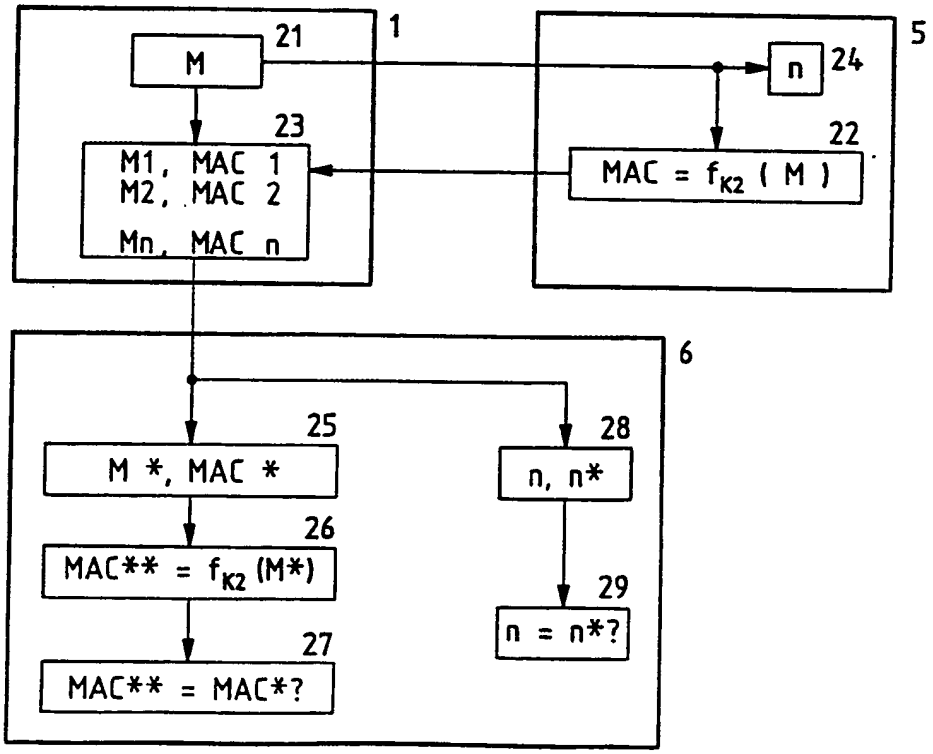

Fig.3